Conclusion

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 juillet 2003 (31.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/063411 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR03/00189

(22) Date de dépôt international :
21 janvier 2003 (21.01.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/00818 23 janvier 2002 (23.01.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : SAGEM SA [FR/FR]; Le Ponant de Paris, 27, rue Leblanc, F-75015 PARIS (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : GOURIO, Cédric [FR/FR]; 149, rue Armand Silvestre, F-92400 Courbevoie (FR).

(74) Mandataires : GORREE, Jean-Michel etc.; Cabinet Plasseraud, 84, rue d'Amsterdam, F-75440 Paris Cedex 9 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: TWO-FACTOR AUTHENTICATION METHOD WITH A ONE-TIME PASSWORD

(54) Titre : PROCEDE D'AUTHENTIFICATION A DEUX FACTEURS AVEC MOT DE PASSE EPHEMERE A USAGE UNIQUE

(57) Abstract: The invention relates to a method of authenticating an information system user. According to the invention, if the user requests access to the information system, said system produces an SMS message containing a limited-duration, one-time password and sends the message to the user's mobile phone which is equipped with a chip card comprising asymmetric key applications and an operating software program. Subsequently, using a data entry means, the user introduces a secret personal code into the mobile phone and submits a personal data support to a read means in the aforementioned phone. Said read means deciphers a private key belonging to the user so that the phone is authorised to decode the SMS message and extract the password from same. Finally, the user sends the password, by means of a transmitting computer terminal, to the information system that authorises user access.

(57) Abrégé : L'invention concerne un procédé d'authentification d'un utilisateur auprès d'un système d'information ; si l'utilisateur demande un accès au système d'information, celui-ci élabore un message SMS contenant un mot de passe à usage unique et à durée de validité limitée et l'envoie à un téléphone mobile, équipé d'une carte à puce avec des applications à clé asymétrique et d'un logiciel d'exploitation, de l'utilisateur; par un moyen d'entrée de données, l'utilisateur introduit un code personnel secret dans le téléphone mobile et soumet un support de données personnel à un moyen de lecture dudit téléphone qui déchiffre une clé privée de l'utilisateur, afin que le téléphone soit autorisé à décoder le message SMS et à en extraire le mot de passe ; enfin l'utilisateur envoie, par un terminal informatique émetteur, le mot de passe à destination du système d'information qui autorise l'accès.

WO 03/063411 A1

PROCEDE D'AUTHENTIFICATION A DEUX FACTEURS AVEC MOT DE PASSE EPHEMERE A USAGE UNIQUE

La présente invention concerne des perfectionnements apportés aux procédés d'authentification, auprès d'un système d'information, d'un utilisateur disposant d'au moins un téléphone mobile qui comprend un moyen d'affichage de données (tel qu'un écran), un moyen d'entrée de données (tel qu'un clavier) et un moyen de lecture d'un support de données (tel qu'une carte à puce).

De nombreux systèmes d'information (base de données, service bancaire, service comptable, réseau privé d'entreprise, ...) demandent aux utilisateurs de s'authentifier à l'aide d'une donnée secrète (nom d'utilisateur, mot de passe, ...) couramment dénommée "code PIN" : Personal Identification Number. L'accès au système d'information n'est conditionné que par la connaissance et l'usage de la donnée secrète. Il s'agit d'une authentification à un seul facteur : ce type d'authentification n'offre qu'une garantie limitée quant à l'identité réelle de la personne requérant l'accès au système d'information et ne peut suffire pour certaines applications sensibles.

L'invention a essentiellement pour objet de proposer un procédé perfectionné d'authentification d'un utilisateur auprès d'un système d'information.

A cette fin, il est proposé un procédé tel que mentionné au préambule qui, selon l'invention, se caractérise

en ce que le téléphone mobile est équipé d'une carte à puce comportant des applications à clé asymétrique et un logiciel pour exploiter ladite clé et

en ce que, lorsque l'utilisateur émet un message de demande d'accès depuis un terminal informatique

émetteur vers le système d'information, ce dernier élabore un message SMS contenant un mot de passe à usage unique et à durée de validité limitée et émet ledit message SMS à destination dudit téléphone mobile de l'utilisateur,

puis l'utilisateur, à l'aide dudit moyen d'entrée de données de son téléphone mobile, introduit un code personnel secret dans ledit téléphone mobile et soumet un support de données personnel audit moyen de lecture du téléphone mobile qui déchiffre une clé privée attribuée à l'utilisateur, afin que ledit téléphone mobile soit autorisé à décoder le susdit message SMS et à en extraire le susdit mot de passe,

et enfin l'utilisateur envoie, par le terminal informatique émetteur, le mot de passe à destination du système d'information qui autorise l'accès de l'utilisateur.

Ainsi, conformément à l'invention, l'authentification s'appuie sur un second facteur qui consiste en la possession d'un moyen personnel d'authentification (carte à puce, appareil électronique, fichier informatique, ...) : l'accès de l'utilisateur au système d'information est conditionné par l'utilisation conjointe de la susdite donnée secrète ou code personnel secret ("code PIN") et du moyen personnel d'authentification.

La mise en œuvre du procédé conforme à l'invention s'appuie sur trois acteurs :

- au moins une base de données publiques contenant l'ensemble des certificats des utilisateurs, le système s'appuyant sur une infrastructure à clés publiques ;
- l'utilisateur équipé d'un téléphone mobile agencé de façon appropriée, typiquement avec une carte SIM (SIMToolkit) fournie avec une bi-clé RSA et une

application permettant, après saisie d'un code secret, de déchiffrer un message SMS reçu, puis de l'afficher;

- et le système d'information auquel l'utilisateur souhaite avoir accès.

Le terminal informatique émetteur peut être par exemple un ordinateur de type PC qui est à la disposition de l'utilisateur.

De façon plus spécifique, le procédé peut mettre en œuvre les étapes qui suivent :

- une autorité de certification attribue, à l'utilisateur, une clé publique K_c et une clé privée k_c,
- l'autorité de certification établit une correspondance biunivoque entre la clé publique K_c de l'utilisateur et l'utilisateur,
- le système d'information établit une correspondance biunivoque entre l'utilisateur et une donnée d'appel à l'aide de laquelle l'utilisateur peut, par ledit terminal informatique émetteur, appeler le système d'information,
- à la suite d'un appel de l'utilisateur provenant dudit terminal informatique émetteur, le système d'information génère le susdit mot de passe à usage unique et à durée de vie limitée et demande à l'autorité de certification la clé publique K_c de l'utilisateur enfermée dans un certificat signé de la clé publique de l'autorité de certification,
- le système d'information constitue le susdit message SMS avec le mot de passe à usage unique et à durée de vie limitée codé avec la clé publique de l'utilisateur,
- et c'est ce message SMS qui est envoyé au téléphone mobile de l'utilisateur.

Là, comme indiqué plus haut, il peut être décodé par mise en œuvre combinée de la donnée secrète (code PIN)

de l'utilisateur et du second moyen d'authentification contenant la clé privée k_c de l'utilisateur qui permet d'ouvrir le certificat renfermant le mot de passe.

Grâce au processus de communication, à l'utilisateur, du mot de passe sous couvert d'un certificat signé par l'autorité de certification, ledit mot de passe ne peut pas être décrypté s'il est intercepté frauduleusement.

C'est lorsqu'il est retransmis, par l'utilisateur, vers le système d'information pour être autorisé à l'accès à celui-ci que le mot de passe peut être intercepté. Mais le mot de passe n'est qu'à usage unique: ayant déjà été utilisé par l'utilisateur, il ne sera plus reconnu une seconde fois par le système d'information. En outre, même si l'utilisateur ne l'a pas employé aussitôt après sa réception, le mot de passe est éphémère (durée de vie limitée, par exemple pour 10 minutes) de sorte que, même s'il finit par être identifié dans le terminal informatique de l'utilisateur, sa durée de vie sera expirée.

Dans la configuration actuelle, le téléphone mobile est, comme indiqué plus haut, équipé d'une carte SIM (SIMToolkit) fournie avec une bi-clé RSA, certifiée par l'autorité de certification, et une application permettant, après saisie d'un code secret, de déchiffrer un message SMS élaboré par le système d'information à destination de l'utilisateur (message constitué du mot de passe éphémère à usage unique), puis de l'afficher.

Grâce à la mise en œuvre de clés asymétriques (c'est-à-dire d'un couple clé publique/clé privée), le processus d'authentification ne nécessite pas, à la différence d'un système à clés symétriques, de relation privilégiée entre le système d'information et

l'utilisateur, mais repose entièrement sur l'autorité de certification.

Ainsi, le mot de passe (ou jeton d'authentification) chiffré avec la clé publique de l'utilisateur est, seul, envoyé sous forme de message SMS pour être traité par l'application SIMToolkit. Le jeton d'authentification ainsi obtenu peut être utilisé pour avoir accès à tout type de service via un canal quelconque: site Internet, accès nomade (PPP), messagerie électronique, ….

Dans un exemple intéressant d'application de l'invention, le mot de passe à usage unique peut être un identifiant temporaire de l'utilisateur, tel que notamment un numéro de carte bancaire virtuel.

L'invention peut également trouver une autre application intéressante dans les téléphones mobiles qui seront équipés des futures cartes WIM pour des connexions à un site WAP (Wireless Application Protocol) : ce sera alors la carte WIM qui renfermera la clé privée de l'utilisateur et qui permettra de décoder le mot de passe reçu par l'utilisateur.

REVENDICATIONS

1. Procédé d'authentification, auprès d'un système d'information, d'un utilisateur disposant d'un téléphone mobile qui comprend un moyen d'affichage de données, un moyen d'entrée de données et un moyen de lecture d'un support de données,

caractérisé

en ce que le téléphone mobile est équipé d'une carte à puce comportant des applications à clé asymétrique et un logiciel pour exploiter ladite clé et

en ce que, lorsque l'utilisateur émet un message de demande d'accès depuis un terminal informatique émetteur vers le système d'information, ce dernier élabore un message SMS contenant un mot de passe à usage unique et à durée de validité limitée et émet ledit message SMS à destination dudit téléphone mobile de l'utilisateur,

puis l'utilisateur, à l'aide dudit moyen d'entrée de données de son téléphone mobile, introduit un code personnel secret dans ledit téléphone mobile et soumet un support de données personnel audit moyen de lecture du téléphone mobile qui déchiffre une clé privée attribuée à l'utilisateur, afin que ledit téléphone mobile soit autorisé à décoder le susdit message SMS et à en extraire le susdit mot de passe,

et enfin l'utilisateur envoie, par le terminal informatique émetteur, le mot de passe à destination du système d'information qui autorise l'accès de l'utilisateur.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comprend les étapes qui suivent :

- une autorité de certification attribue, à l'utilisateur, une clé publique K_c et une clé privée k_c,

- l'autorité de certification établit une correspondance biunivoque entre la clé publique K_c de l'utilisateur et l'utilisateur,
- le système d'information établit une correspondance biunivoque entre l'utilisateur et une donnée d'appel à l'aide de laquelle l'utilisateur peut, par ledit terminal informatique émetteur, appeler le système d'information,
- à la suite d'un appel de l'utilisateur provenant dudit terminal informatique émetteur, le système d'information génère le susdit mot de passe à usage unique et à durée de vie limitée et demande à l'autorité de certification la clé publique K_c de l'utilisateur enfermée dans un certificat signé de la clé publique de l'autorité de certification,
- le système d'information constitue le susdit message SMS avec le mot de passe à usage unique et à durée de vie limitée codé avec la clé publique de l'utilisateur,
- et c'est ce message SMS qui est envoyé au téléphone mobile de l'utilisateur.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le mot de passe à usage unique est un identifiant temporaire attribué temporairement à l'utilisateur.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/00189

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F G07F H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 881 559 A (SIEMENS AG) 2 December 1998 (1998-12-02) page 5, line 51 -page 6, line 31	1
A	page 7, line 17 - line 30 page 14, line 33 - line 42	2
A	OMURA J K: "NOVEL APPLICATIONS OF CRYPTOGRAPHY IN DIGITAL COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER. PISCATAWAY, N.J, US, vol. 28, no. 5, 1 May 1990 (1990-05-01), pages 21-29, XP000132493 ISSN: 0163-6804 page 25, left-hand column, line 1 -page 26, left-hand column, line 2; figure 4 page 28, left-hand column, line 30 -right-hand column, line 12; figure 8	1

-/—

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 May 2003	27/05/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/00189

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ROTRAUT LAUN: "ASYMMETRIC USER AUTHENTICATION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 11, no. 2, 1 April 1992 (1992-04-01), pages 173-183, XP000245841 ISSN: 0167-4048 page 173, left-hand column, line 12 -page 174, left-hand column, line 28 page 178, left-hand column, line 3 -right-hand column, line 16; figure 2 page 181, left-hand column, line 15 -right-hand column, line 30	1,2
Y	WO 01 80525 A (SUN MICROSYSTEMS INC) 25 October 2001 (2001-10-25) abstract page 3, line 30 -page 9, line 4; figure 6	1
A	WO 01 92999 A (CITRIX SYSTEMS INC) 6 December 2001 (2001-12-06) abstract page 4, line 11 -page 10, line 3; figures 1,2	1
A	NL 1 007 409 C (NEDERLAND PTT) 18 November 1997 (1997-11-18) the whole document	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/00189

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0881559	A	02-12-1998	EP	0881559 A1	02-12-1998
			CN	1207530 A	10-02-1999
			US	6047242 A	04-04-2000
WO 0180525	A	25-10-2001	AU	4529201 A	30-10-2001
			WO	0180525 A1	25-10-2001
WO 0192999	A	06-12-2001	AU	6478601 A	11-12-2001
			WO	0192999 A2	06-12-2001
NL 1007409	C	18-11-1997	NL	1007409 C1	18-11-1997

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/00189

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G06F G07F H04Q

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 881 559 A (SIEMENS AG) 2 décembre 1998 (1998-12-02) page 5, ligne 51 -page 6, ligne 31	1
A	page 7, ligne 17 - ligne 30 page 14, ligne 33 - ligne 42	2
A	OMURA J K: "NOVEL APPLICATIONS OF CRYPTOGRAPHY IN DIGITAL COMMUNICATIONS" IEEE COMMUNICATIONS MAGAZINE, IEEE SERVICE CENTER. PISCATAWAY, N.J, US, vol. 28, no. 5, 1 mai 1990 (1990-05-01), pages 21-29, XP000132493 ISSN: 0163-6804 page 25, colonne de gauche, ligne 1 -page 26, colonne de gauche, ligne 2; figure 4 page 28, colonne de gauche, ligne 30 -colonne de droite, ligne 12; figure 8	1

-/—

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
19 mai 2003	27/05/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dujardin, C

1

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	ROTRAUT LAUN: "ASYMMETRIC USER AUTHENTICATION" COMPUTERS & SECURITY. INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, ELSEVIER SCIENCE PUBLISHERS. AMSTERDAM, NL, vol. 11, no. 2, 1 avril 1992 (1992-04-01), pages 173-183, XP000245841 ISSN: 0167-4048 page 173, colonne de gauche, ligne 12 -page 174, colonne de gauche, ligne 28 page 178, colonne de gauche, ligne 3 -colonne de droite, ligne 16; figure 2 page 181, colonne de gauche, ligne 15 -colonne de droite, ligne 30	1,2
Y	WO 01 80525 A (SUN MICROSYSTEMS INC) 25 octobre 2001 (2001-10-25) abrégé page 3, ligne 30 -page 9, ligne 4; figure 6	1
A	WO 01 92999 A (CITRIX SYSTEMS INC) 6 décembre 2001 (2001-12-06) abrégé page 4, ligne 11 -page 10, ligne 3; figures 1,2	1
A	NL 1 007 409 C (NEDERLAND PTT) 18 novembre 1997 (1997-11-18) le document en entier	1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/00189

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0881559	A	02-12-1998	EP	0881559 A1	02-12-1998
			CN	1207530 A	10-02-1999
			US	6047242 A	04-04-2000
WO 0180525	A	25-10-2001	AU	4529201 A	30-10-2001
			WO	0180525 A1	25-10-2001
WO 0192999	A	06-12-2001	AU	6478601 A	11-12-2001
			WO	0192999 A2	06-12-2001
NL 1007409	C	18-11-1997	NL	1007409 C1	18-11-1997